CRITICAL INFRASTRUCTURE DEVELOPMENTS

July 15, 1999
Issue 9♦99

- **Back Orifice 2000: Def Con Conference Preview**
- **Low Bandwidth Attacks: New Computer Intruder Reconnaissance Tactic**
- **Social Engineering & Cyber Threat: Lessons from a Failed Attempt**

This publication provides information on current critical infrastructure protection issues, with emphasis on computer and network security matters.

Analytical commentary within is identified in **bold** text.

We welcome your comments and suggestions for improving this product. For more information, or to provide comments, please contact the NIPC Watch at **nipc.watch@fbi.gov** or call (202) 324-0340.

Back Orifice 2000: Def Con Conference Preview

By Edward E. Barr

The new version of the hacker tool Back Orifice has new capabilities and is Windows NT compatible.

A new version of the popular hacker tool Back Orifice was previewed on July 10th at the Def Con VII hacker conference in Las Vegas. Back Orifice 2000, also known as BO2K, has several new capabilities, the most important of which is its compatibility with Windows NT. The original version of Back Orifice did not run on NT, which left a considerable number of computers immune to the threat. Now that NT is vulnerable to Back Orifice, all current versions of Windows operating systems can be exploited by this simple-to-use, graphical user interface hacker tool. Other new features include an open plug-in architecture, which will allow third parties to create add-ons that further increase the malicious capability of BO2K, strong cryptography to keep network communications secure and open source code. BO2K is free and will be available for download soon.

BO2K was created by the hacker group, Cult of the Dead Cow, which considers BO2K a professional remote control tool for system administrators. Back Orifice is a pun of the Microsoft Back Office server suite.

The original version of Back Orifice was extremely effective in compromising Windows 95, and 98 operating systems. The original Back Orifice tool compromised thousands of computers and, now that it can compromise NT as well, many more machines are likely to fall victim to BO2K. As of this writing, however, no US computer system compromises have been reported to the FBI. Anti-virus software vendors are working on patches that will allow their software to detect and remove BO2K, and CERT is preparing an advisory on the new tool.

Low Bandwidth Attacks: New Computer Intruder Reconnaissance Tactic

By Edward E. Barr

Hackers are using "low-bandwidth attacks," a new tactic to scan and probe computer systems. This new technique reduces the intruder's risk of detection by network security countermeasures.

The new tactic of "low-bandwidth attacks" sends a low volume, intermittent series of scanning or probing packets from various locations. These "low-bandwidth attacks" may consist of several hackers from different locations agreeing to work together to scan and probe systems for vulnerabilities. In contrast, conventional scanning and probing methods consist of sending large numbers of packets from a single location. Because this new method does not send a flood of packets from a single location, it is often below the detection threshold of most firewalls and intrusion detection systems. Some documented "low-bandwidth attacks" have sent only a few packets per hour, from five different sources; others have used 15 different IP addresses from one country.

The US Navy has documented the new tactic. Although it is possible for one person to conduct such activity from multiple sites, the US Navy believes that groups of individuals are working together to conduct this reconnaissance. Part of the rationale for this conclusion is based on slight variances in how scans are conducted and the multiple hardware/OS platforms used. This would indicate a new level of cooperation among network intruders.

Until network intrusion systems are upgraded to detect this type of activity, network administrators can insulate their systems from scans and probes by keeping internal IP addresses hidden behind firewalls and proxy servers. In addition, one indication that a system has been a victim of a low-bandwidth attack is attempted connections to nonexistent services. System administrators can review their logs for this type of activity.

Social Engineering & Cyber Threat: Lessons from a Failed Attempt

By Domokos Hajdo

A recent failed social engineering attempt at a US company shows that threats to the US critical infrastructures may take many forms and illustrates the need for industry policies and practices to supplement physical and electronic security measures.

Recently, the duty supervisor at a US critical infrastructure company received a call from a man claiming to be a technician from a trusted vendor company. The technician explained that he needed access to the supervisor's facility in order to perform a software upgrade. Yet the caller was evasive, at first, when asked who had authorized the visit. He offered a name, but the duty supervisor knew that no such employee existed. When challenged, the caller offered a valid employee name, but a quick phone call to that employee revealed that no technicians were expected. An hour later, the caller tried the same approach with a second duty supervisor, who also denied the request. No technician ever arrived at the company, the caller never repeated the attempt, and the chief of security for the company notified his local FBI field office.

In this instance, everyone at the company acted properly in response to an apparent social engineering attempt. But the social engineer in this case was not particularly skilled or prepared. Other, more infamous, convicted intruders have spent months meticulously mapping out company organization charts, forging identification cards, obtaining uniforms, and using other means to dupe personnel at target companies. Had the potential intruders successfully employed such tactics, their access to sensitive industry computer systems alone could have given them the opportunity to steal, modify, or destroy information; otherwise disrupt operations; monitor communications; or implant malicious code, such as software logic bombs that at a certain date or upon receipt of a remote signal shut off power generation.

This recent incident illustrates that individuals continue to use physical intrusion attempts as a means to penetrate corporate information systems at critical US industries. The incident also points out that physical and electronic security measures alone are insufficient to protect against the threat. Industry security policies, practices, and training need to highlight the methods used by social engineers and the potential for serious security compromises.